

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

**IN THE MATTER OF THE SEARCH OF:
ONE RESIDENCE AND ONE PERSON
INCLUDING ANY AND ALL MOBILE
DIGITAL DEVICES OWNED, USED, OR
CONTROLLED BY THAT PERSON
UNDER RULE 41**

SW No. 24-mj-52-01-AJ

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE**

I, Malachi C. Nkosi, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 6 Blackberry Road, Apartment B, Derry, New Hampshire, hereinafter “PREMISES,” further described in Attachment A, for the things described in Attachment B.

2. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, that statement is described in substance and is not intended to be a verbatim recitation of such statement. Wherever in this affidavit I quote statements, those quotations have been taken from draft transcripts, which are subject to further revision.

3. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I’ve drawn from my training, experience, and knowledge of the investigation.

AFFIANT BACKGROUND

4. I am a Special Agent with Federal Bureau of Investigation (“FBI”). I have been in this position since August 2020. I am currently assigned to the Philadelphia Joint Terrorism Task Force in the FBI Philadelphia Field Office. In my duties as a Special Agent, I have investigated various violations of federal law including riots and acts of violence in furtherance of a riot. Currently, I am tasked with investigating criminal activity in and around the United States Capitol grounds on January 6, 2021. As such, I am an “investigative or law enforcement officer” of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1752(a)(1) and (b)(1)(A) (Entering and Remaining in Restricted Building or Grounds with a Deadly or Dangerous Weapon); 18 U.S.C. § 1752(a)(2) and (b)(1)(A) (Disorderly and Disruptive Conduct in a Restricted Building or Grounds with a Deadly or Dangerous Weapon); and 40 U.S.C. §§ 5104(e)(2)(D) (Disorderly or Disruptive conduct in a Capitol Building) and 5104(e)(2)(G) (Parading, Demonstrating, or Picketing in a Capitol Building) (the “TARGET

OFFENSES”) that have been committed by Charles Anthony Espinosa (the “Subject”) and other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, the Subject, as well as others observed by the Subject. There is also probable cause to search the PREMISES, further described in Attachment A, for the things described in Attachment B.

PROBABLE CAUSE

Background – The U.S. Capitol on January 6, 2021

7. U.S. Capitol Police (USCP), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred on January 6, 2021, at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510.

8. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

9. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, two staircases, and multiple terraces. On the east side of the Capitol is the East Front, which includes three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor’s Center surrounded by a concrete parkway. All of this area was barricaded and closed to members of the public on January 6, 2021.

10. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of Representatives and the United States Senate were meeting to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020

(“Certification”). The joint session began at approximately 1:00 p.m. Eastern Standard Time¹ in the House of Representatives. Shortly thereafter, by approximately 1:30 p.m., the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

11. The grounds around the Capitol were posted and cordoned off, and the entire area as well as the Capitol building itself were restricted as that term is used in Title 18, United States Code, Section 1752 due to the fact that the Vice President and the immediate family of the Vice President, among others, would be visiting and did visit the Capitol complex that day.

12. At around 1:00 p.m., individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol. As a result of these and other similar actions by the crowd, the situation at the Capitol became a civil disorder as that term is used in Title 18, United States Code, Section 231. The civil disorder obstructed the ability of the U.S. Secret Service to perform the federally protected function of protecting Vice President Pence.

13. As they advanced unlawfully onto Capitol grounds and towards the U.S. Capitol building over the next several hours, individuals in the crowd destroyed barricades and metal fencing and assaulted law enforcement officers with fists, poles, thrown objects, and chemical irritant sprays, among other things. Individuals in the crowd carried weapons including tire irons, sledgehammers, bear spray, and tasers, some of which were also used to assault members of law enforcement. A number of individuals in the crowd wore tactical vests, helmets, and respirators.

¹ All times stated in this affidavit are in Eastern Time unless otherwise noted.

14. At approximately 2:00 p.m., some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured.

15. Beginning shortly after 2:00 p.m., individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement.

16. Once inside, certain of the unlawful entrants destroyed property, stole property, and assaulted federal police officers.

17. Between approximately 2:10 p.m., and 2:30 p.m., Vice President Pence evacuated the Senate Chamber, and the Senate and House of Representatives went into recess. Unlawful entrants into the U.S. Capitol building attempted to break into the House chamber by breaking the windows on the chamber door. Law enforcement officers inside the House of Representatives drew their weapons to protect members of the House of Representatives who were stuck inside. Both the Senate and the House of Representatives Chamber were eventually evacuated.

18. At around 2:47 p.m., subjects broke into the Senate Chamber not long after it had been evacuated.

19. At around 2:48 p.m., DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m. Mayor Bowser's order imposing a curfew in the District of Columbia impacted interstate commerce. For example, grocery store Safeway closed all 12 of its stores in the District of Columbia as of 4 p.m. that day, and Safeway's stores were supposed to close at 11 p.m.

20. At about 3:25 p.m., law enforcement officers cleared the Senate floor. Between 3:25 and around 6:30 p.m., law enforcement was able to clear the U.S. Capitol of all of the subjects.

21. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the danger posed by individuals who had entered the U.S. Capitol without any security screening, the joint session could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol throughout the events, including during the time he was evacuated from the Senate Chamber until the joint session concluded at approximately 3:44 a.m. on January 7, 2021.

22. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

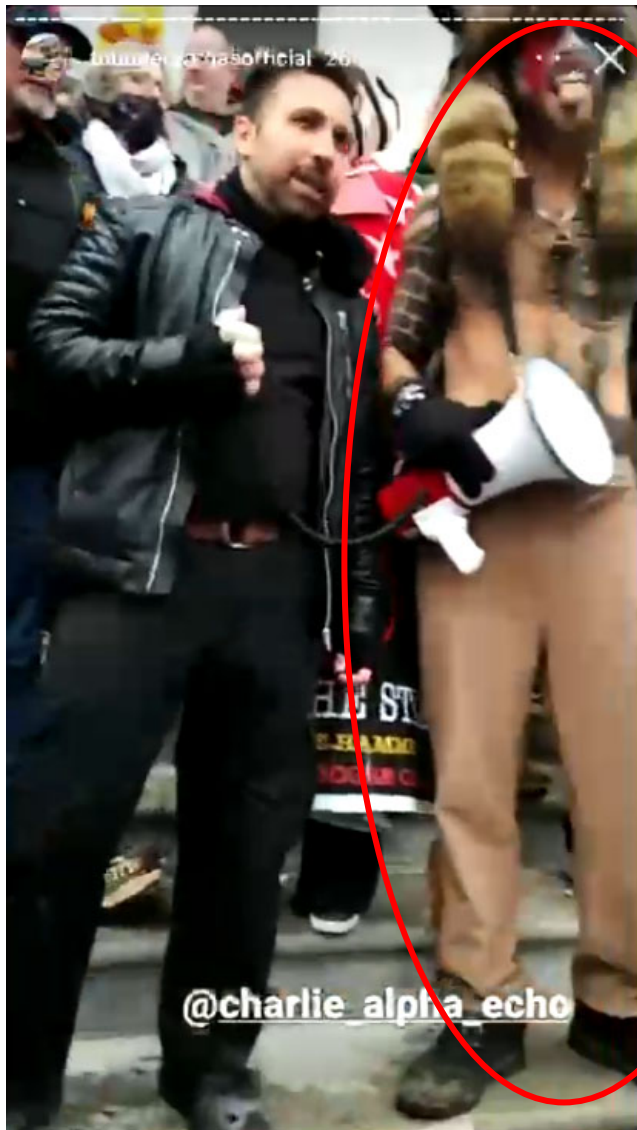
23. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

24. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

Facts Specific to This Application

25. On or about January 23, 2021, the FBI received an online tip via the FBI National Threat Operations Center (“NTOC”) that CHARLES ANTHONY ESPINOSA (“ESPINOSA”) was in and around the U.S. Capitol building and grounds on January 6, 2021. Specifically, a confidential witness (“CW-1”) provided information that CW-1 had seen social media photos and videos via an Instagram account associated with ESPINOSA, showing ESPINOSA inside the U.S. Capitol building and on the U.S. Capitol grounds on January 6, 2021. CW-1 further provided a video showing ESPINOSA around the U.S. Capitol grounds on January 6, 2021.

26. The FBI then identified additional third party footage and social media postings which also placed ESPINOSA inside and around the U.S. Capitol building and grounds on January 6, 2021. The FBI compared known photographs of ESPINOSA obtained from law enforcement databases to the images and videos depicted below. A substantial amount of the social media depicting ESPINOSA on January 6, 2021 was posted by the Instagram username “Charlie_alpha_echo.” One video tagging “Charlie_alpha_echo” showed ESPINOSA on the steps of the Capitol speaking to the crowd (through a megaphone held by another rioter) saying, “I think this should be happening in every single major city in the country.”



(Image 1: still from Instagram video taken on January 6, 2021)

27. Instagram provided the FBI with subscriber information for the Instagram account “Charlie_alpha_echo.” “Charlie,” “alpha,” and “echo,” are common symbols in the phonetic alphabet used to denote the letters “C,” “A,” and “E,” which are ESPINOSA’s initials.

28. On January 3, 2023, Agents reviewed a public, unrestricted post on ESPINOSA’s Instagram Account featuring a “selfie” of ESPINOSA holding a black Apple iPhone, which

appears to be similar to the device ESPINOSA used when inside and outside the United States Capitol building on January 6, 2021.



(Image 2: screenshot of ESPINOSA posted to Instagram account “charlie_alpha_echo”)

29. The FBI further connected the “Charlie_alpha_echo” Instagram account to ESPINOSA through the subscriber phone number and email account used to register with Instagram. Specifically, the Instagram account “Charlie_alpha_echo” corresponded to a telephone number ending in 2841² (hereinafter “SUBJECT PHONE NUMBER”) and an email address (hereinafter “SUBJECT EMAIL”)—both associated with ESPINOSA through subscriber information from AT&T. AT&T, the service carrier for SUBJECT PHONE NUMBER,

² This phone number and subsequent email address are known in full to the affiant.

provided subscriber information, indicating that SUBJECT PHONE NUMBER was attributed exclusively to ESPINOSA. AT&T further provided a billing address and SUBJECT EMAIL, which law enforcement confirmed are both associated with ESPINOSA.

30. According to records obtained through a search warrant which was served on AT&T, on January 6, 2021, in and around the time of the incident, the cellphone associated with the SUBJECT PHONE NUMBER was identified as having utilized a cell site consistent with providing service to a geographic area that includes the interior of the United States Capitol building.

31. ESPINOSA'S previous employer provided attendance records for ESPINOSA. Per his employer's records, ESPINOSA requested paid time off for January 6, 2021 and January 7, 2021. In the leave request comments section for January 7, 2021, ESPINOSA submitted: "Stop the steal!"

32. Records obtained from the Westin Hotel in Washington, D.C. confirm that ESPINOSA booked a room at the hotel through Expedia.com, with an arrival date of January 5, 2021 and a departure date of January 7, 2021. The Westin Hotel confirmed that ESPINOSA stayed there the entirety of his reservation, and gave a specific room number in which ESPINOSA stayed. The Westin Hotel also provided information reflecting that ESPINOSA checked in at approximately 8:28 p.m. local time on January 5, 2021 and checked out at approximately 2:36 p.m. local time on January 7, 2021. According to records provided by the Westin Hotel, ESPINOSA used the SUBJECT EMAIL referenced above, which is confirmed to be associated with ESPINOSA.

33. While in Washington, D.C., ESPINOSA traveled to the U.S. Capitol on January 6, 2021. Specifically, ESPINOSA entered the restricted area on U.S. Capitol grounds and also

entered the Capitol building. As part of its investigation, the FBI reviewed third party video uploaded to YouTube on or about January 7, 2021 titled “United States Capitol Protest January 6th, 2021” (https://www.youtube.com/watch?v=O_vrdc4V3aY&t=81s). At timestamp 1:21, the video shows ESPINOSA walking over a downed fence with clearly marked “AREA CLOSED” signs posted at regular intervals across the fence. (See Image 2 below.) In this video, ESPINOSA walks over the fallen fence after it was torn to the ground, with parts of the fence still intact surrounding the restricted area. In this video, as well as the following images and videos from January 6, 2021, ESPINOSA is seen wearing the same material and clothing—leather jacket over a red hoodie, black jeans, black shoes, fingerless gloves—consistent with other footage of ESPINOSA in and around the United States Capitol building on January 6, 2021.



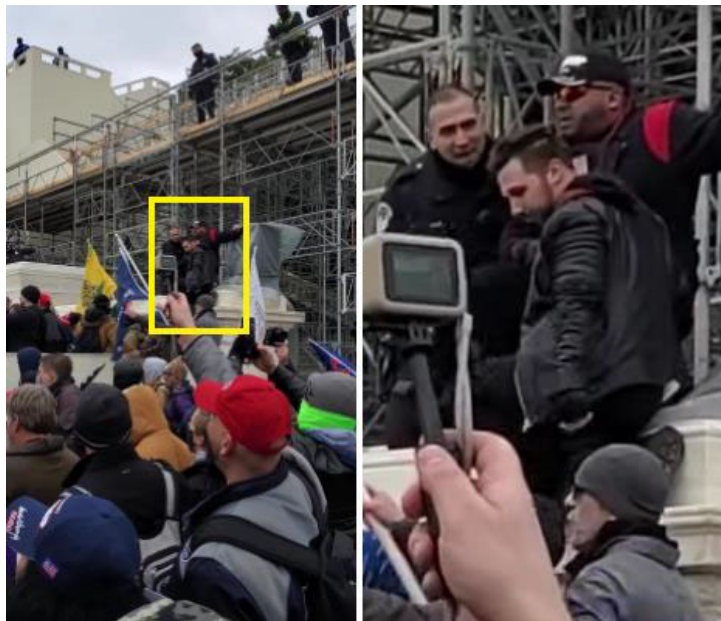
(Image 3: still from Youtube video taken on January 6, 2021)

34. The FBI further reviewed a third-party video uploaded to YouTube on or about January 8, 2021 titled “FULL FOOTAGE: Patriots STORM U.S. Capitol (4K60fps)” (<https://www.youtube.com/watch?v=iNFcdpZdkh0&t=702s>). At timestamp 11:42, the video shows ESPINOSA turning back to look at the camera that was recording this video, showing his face without a face mask. ESPINOSA is wearing the same material and clothing consistent with other footage of him in and around the United States Capitol building on January 6, 2021.



(Image 4: still from Youtube video taken on January 6, 2021)

35. The FBI further reviewed a YouTube video uploaded to YouTube on or about January 06, 2021 titled “patriots storm capitol” (<https://www.youtube.com/watch?v=r1owIQzOYU0&t=465s>). At timestamp 7:45, the video shows ESPINOSA standing next to the scaffolding, near the United States Capitol building.



(Image 5: still from Youtube video taken January 6, 2021)

36. The FBI also reviewed a third-party video uploaded to [gettyimages.com](https://www.gettyimages.com/detail/video/police-say-they-have-bolstered-security-in-washington-news-footage/1306269489) (<https://www.gettyimages.com/detail/video/police-say-they-have-bolstered-security-in-washington-news-footage/1306269489>). At timestamp 1:06, the video shows ESPINOSA using a bike rack to climb up a wall of the Capitol building with the help of other rioters. ESPINOSA climbed onto the Lower West Terrace of the United States Capitol building, wearing the material and clothing consistent with earlier sightings of him in and around the United States Capitol building on January 6, 2021.



(Image 6: still from gettyimages footage taken on January 6, 2021)

37. The FBI also reviewed a YouTube video uploaded to YouTube on or about January 14, 2021 titled “Photographer, Brendan Gutenschwager, shares video of siege on the US Capitol” (<https://www.youtube.com/watch?v=gTurnetBh4A&t=796>). At timestamp 13:15, the video shows ESPINOSA entering the United States Capitol Building and holding a black cellphone in front of him, in what appeared to be him taking a photo or recording a video.



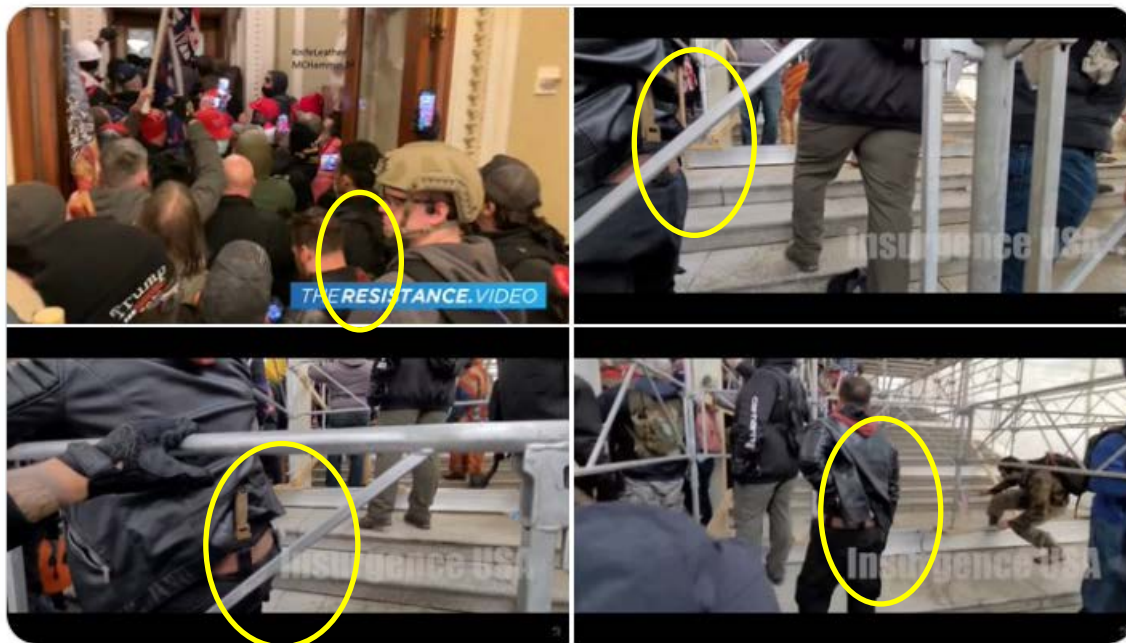
(Image 7: still from YouTube video taken January 6, 2021)

38. The FBI also reviewed a [gettyimages.com](http://gettyimages.com/detail/1294949353) video uploaded to gettyimages (<http://gettyimages.com/detail/1294949353>). At timestamp 0:35, the video shows ESPINOSA inside the United States Capitol building—specifically pushing up to the door of the U.S. House of Representatives.



(Image 8: still from gettyimages.com video taken January 6, 2021)

39. The FBI further reviewed unrestricted, public social media posts on the Twitter (or X) social media platform using the search “#KnifeLeather.” The hashtag identifier “#KnifeLeather” was associated with ESPINOSA in open source research and provided media of ESPINOSA wearing material consistent with earlier sightings of him in and around the United States Capitol building on January 6, 2021. This material was posted by Twitter users using the “#KnifeLeather” tag in their posts with dates ranging from approximately February 2021 to September 2022. These posts contained multiple images of ESPINOSA outside and inside the U.S. Capitol building on January 6, 2021. Additionally, some of these posts contained pictures of ESPINOSA with what appeared to be a large knife concealed in the rear waistband of his pants, underneath his black leather jacket. In some of the following images, ESPINOSA appears to be underneath scaffolding on the west front of the U.S. Capitol on January 6, 2021, within the restricted area, while in possession of a large knife.

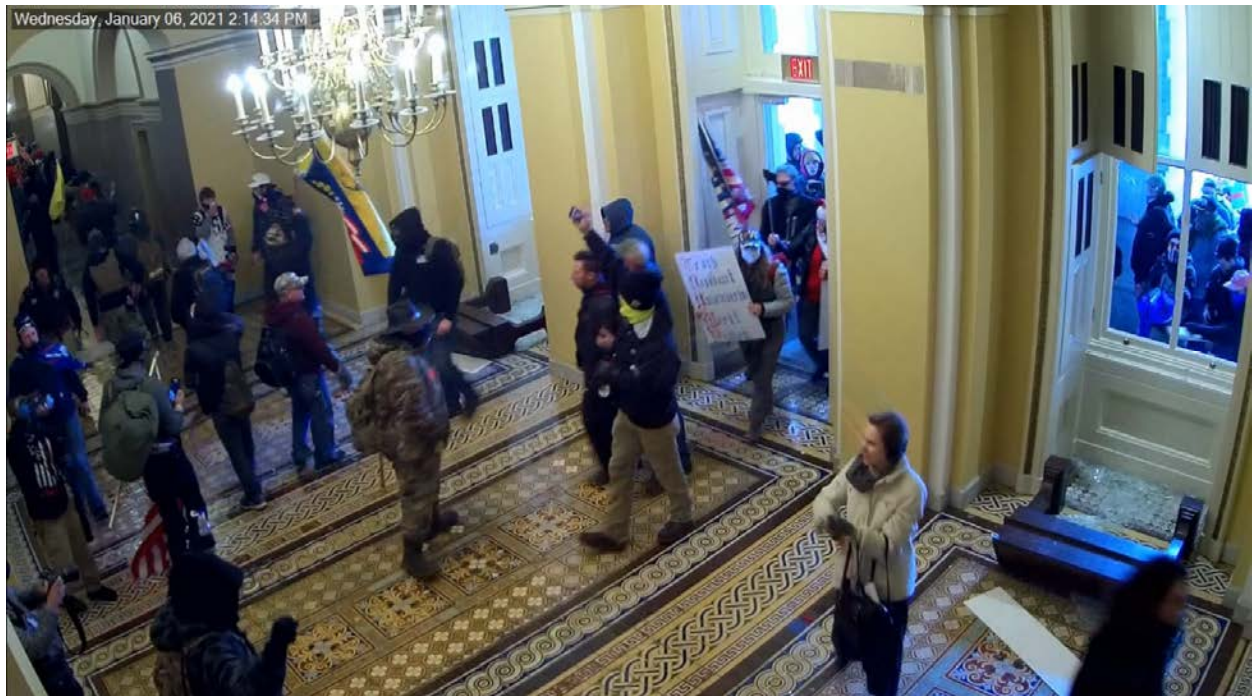


(Image 9: re-posted third party images taken January 6, 2021, of which the top left, and bottom two photos visibly show the knife)



(Image 10: re-posted third party images taken January 6, 2021)

40. As captured by U.S. Capitol Police surveillance footage, at approximately 2:14:34 p.m. EST, ESPINOSA entered the United States Capitol building through the Senate Wing door via the west side of the U.S. Capitol building.



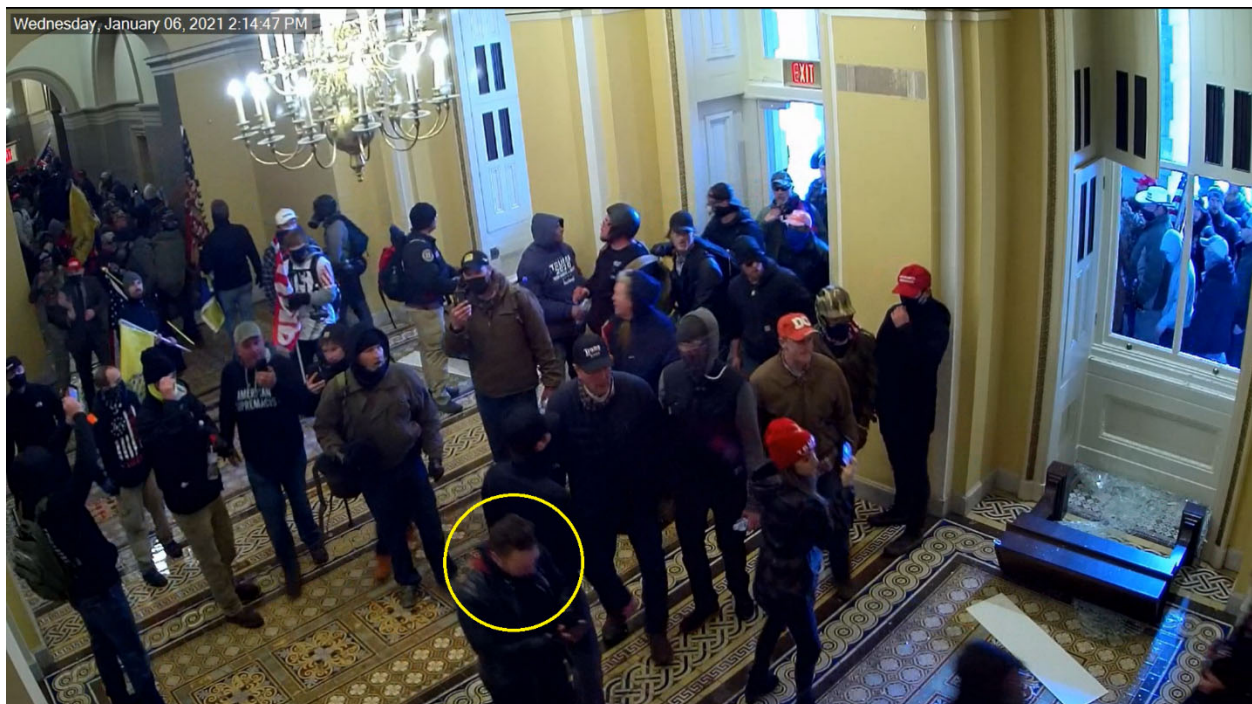
(Image 11: U.S. Capitol Police surveillance footage taken January 6, 2021)

41. After initially heading to the right upon entering the U.S. Capitol through the Senate Wing door, ESPINOSA changed course and made his way to the left of the Senate Wing door.



(Image 12: U.S. Capitol Police surveillance footage taken January 6, 2021)

42. At approximately 2:14:47 p.m. EST, ESPINOSA took out what appeared to be a cell phone from his front left inside jacket pocket and appeared to be looking at the cell phone as he entered further into the U.S. Capitol building.



(Image 13: U.S. Capitol Police surveillance footage taken January 6, 2021)

43. ESPINOSA returned to his original entry point at approximately 2:15:26 p.m. EST, while wearing a face mask.



(Image 14: U.S. Capitol Police surveillance footage taken January 6, 2021)

44. At approximately 2:15:29 p.m. EST, ESPINOSA lowered his face mask, making his face visible.



(Image 15: U.S. Capitol Police surveillance footage taken January 6, 2021)

45. At approximately 2:15:56 p.m. EST, ESPINOSA walked to the opposite side of the Senate Wing door entryway inside the U.S. Capitol and leaned up against the wall inside the Capitol building as other rioters streamed inside through the Senate Wing door. ESPINOSA appeared to be using his cellphone as he leaned against the wall.



(Image 16: U.S. Capitol Police surveillance footage taken January 6, 2021)

46. At approximately 2:19:34 p.m. EST, additional security surveillance footage, capturing the North Crypt sector of the Capitol building, captured ESPINOSA entering from the far right of the camera view into the Crypt and approaching a statue with his face mask lowered.



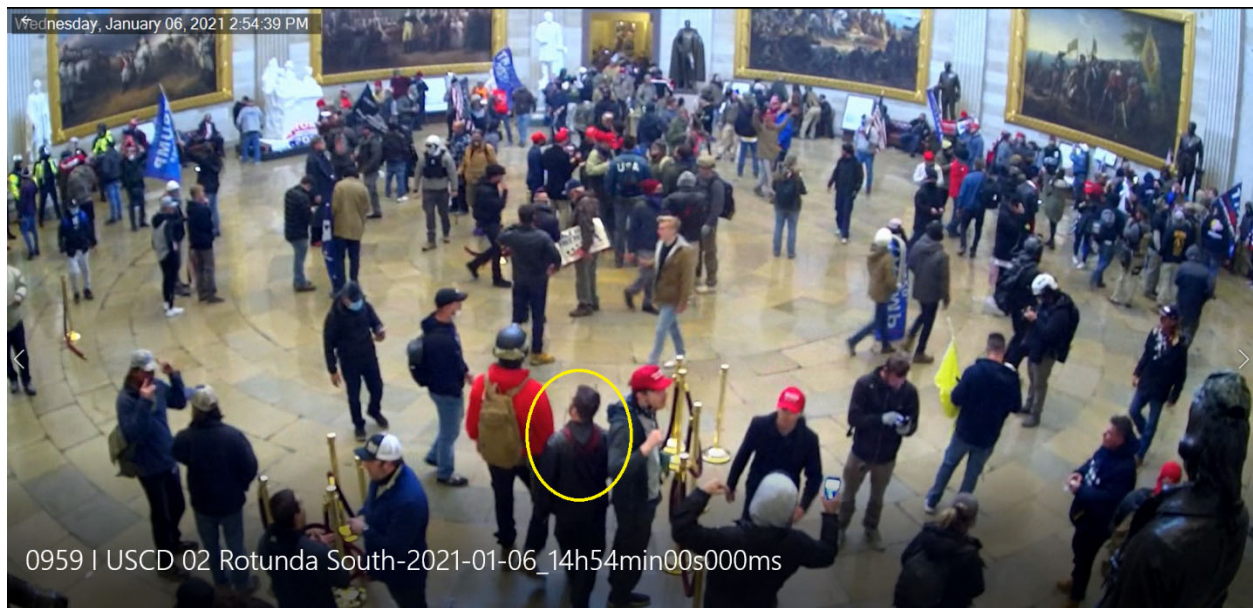
(Image 17: U.S. Capitol Police surveillance footage taken January 6, 2021)

47. At approximately 2:26 p.m. EST, additional surveillance footage from the U.S. Capitol Police showed ESPINOSA continue to use a cell phone as he walked through the Crypt.



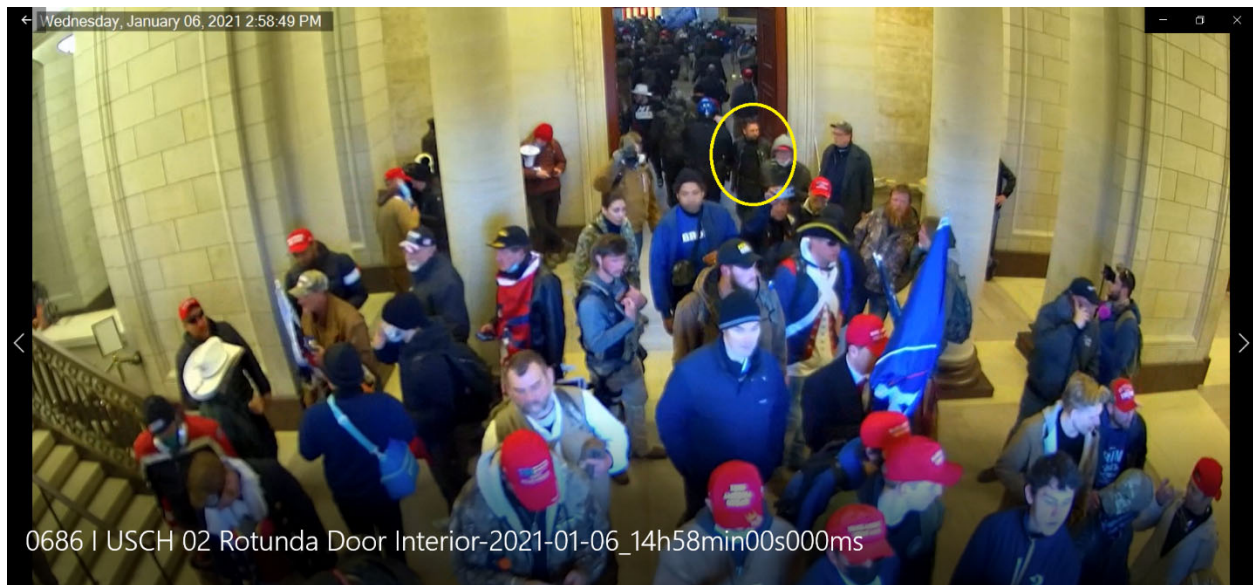
(Image 18: U.S. Capitol Police surveillance footage taken January 6, 2021)

48. At approximately 2:54:39 p.m. EST, ESPINOSA entered the Rotunda of the U.S. Capitol Building. Additional video showed ESPINOSA walk to the upper right corner and use a cell phone again. ESPINOSA remained in the Rotunda for approximately three minutes.



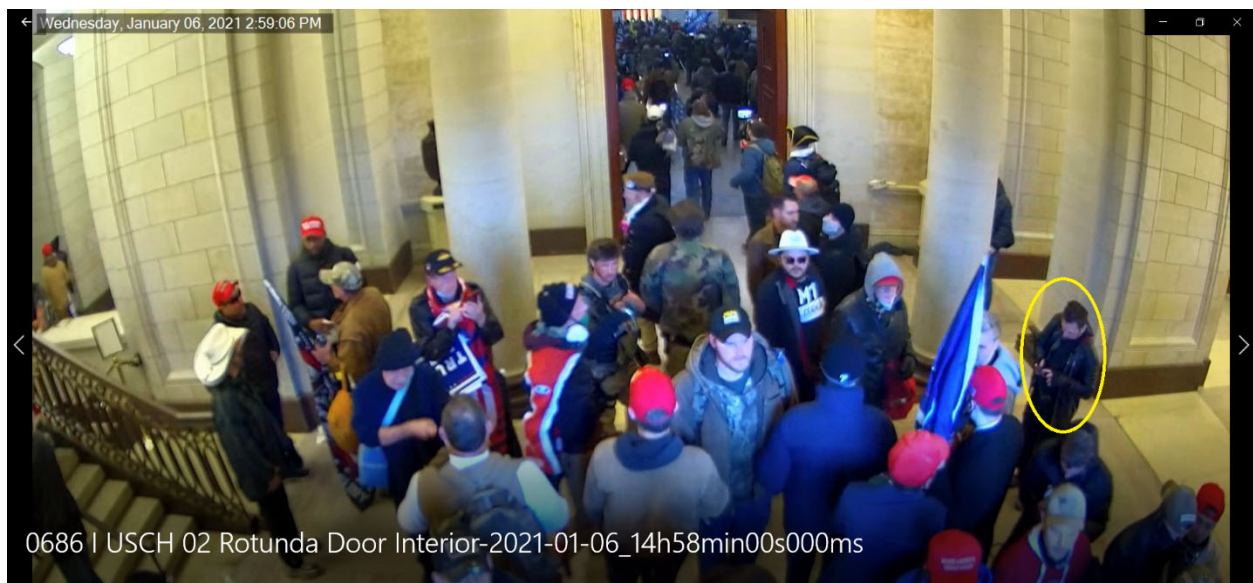
(Image 19: U.S. Capitol Police surveillance footage taken January 6, 2021)

49. At approximately 2:58:49 p.m. EST, ESPINOSA exited the Rotunda and made his way toward the East Rotunda door—on the opposite side of the U.S. Capitol from where he had originally entered from the west front.



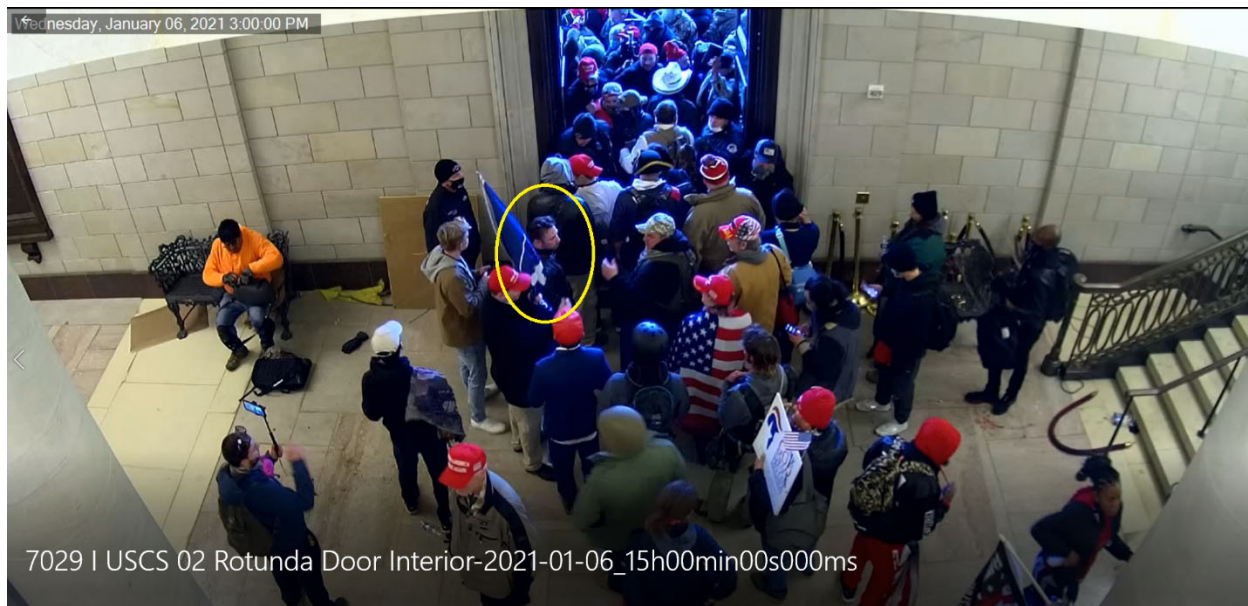
(Image 20: U.S. Capitol Police surveillance footage taken January 6, 2021)

50. At approximately 2:59:06 p.m. EST, ESPINOSA stops inside the East Rotunda door to use his cell phone.



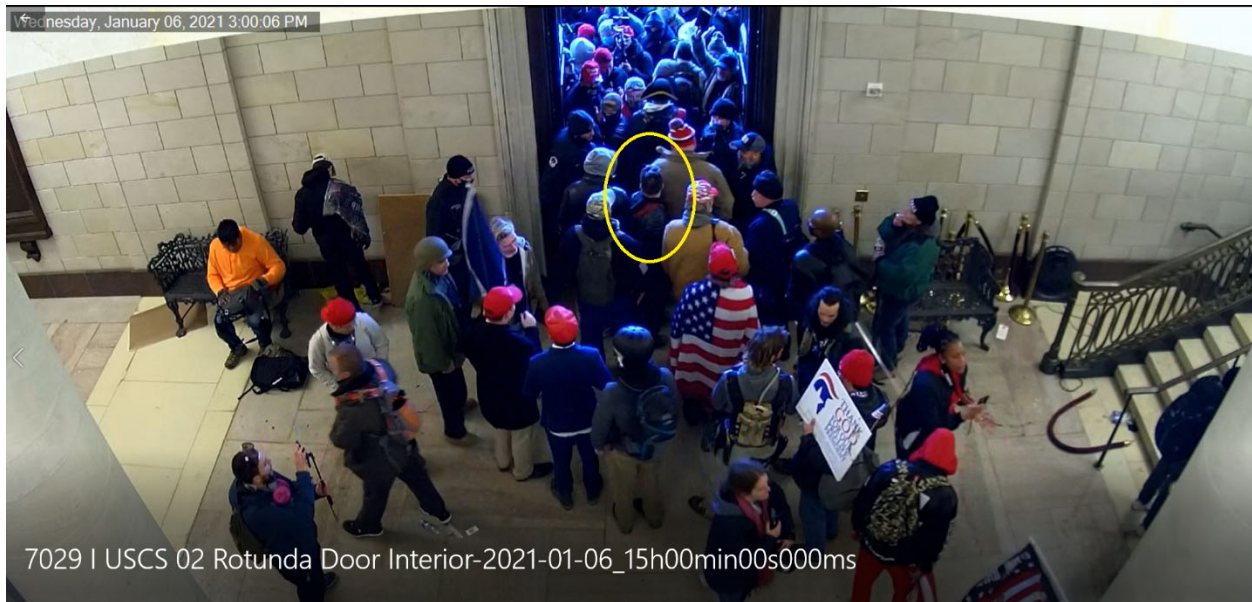
(Image 21: U.S. Capitol Police surveillance footage taken January 6, 2021)

51. At approximately 3:00 p.m. EST, ESPINOSA begins to leave the U.S. Capitol through the East Rotunda door, exiting toward the east front of the U.S. Capitol.



(Image 22: U.S. Capitol Police surveillance footage taken January 6, 2021)

52. At approximately 3:00:06 p.m. EST, ESPINOSA exited the United States Capitol Building.



(Image 23: U.S. Capitol Police surveillance footage taken January 6, 2021)

53. There is also probable cause to search the PREMISES, further described in Attachment A, for the things described in Attachment B.

54. On February 22, 2024, the FBI conducted physical surveillance of the PREMISES. At approximately 4:46 a.m., FBI agents observed multiple vehicles at the PREMISES, including a Kia Sorrento with New Hampshire license plate number 5157780, which was parked in the driveway of the PREMISES on the right side of the residence. The FBI confirmed that this vehicle is registered to ESPINOSA. FBI observed the same vehicle registered to ESPINOSA parked at the PREMISES on March 8, 2024 and March 11, 2024.

55. On March 11, 2024, between the hours of 6:20 a.m. and 7:05 a.m. the FBI saw an individual agents identified ESPINOSA, who was driving the Kia Sorrento with New Hampshire license plate number 5157780 away from the PREMISES after it had been parked at the PREMISES.

56. FBI confirmed through the U.S. Postal Service that, as of February 12, 2024, ESPINOSA has been receiving parcels addressed to the PREMISES.

57. Based upon the surveillance conducted by FBI and the registration of the Subject to receive parcels at the PREMISES there is probable cause to believe that the PREMISES is ESPINOSA's current residence.

58. Your affiant also knows that hundreds of people have been arrested in connection to the riot that occurred at the U.S. Capitol on January 6, 2021. During searches of many of those people's residences, from early 2021 through present, in multiple jurisdictions, law enforcement has recovered clothing, paraphernalia, tools, and devices that were worn, used, or carried on January 6, 2021. Items from the events of January 6, 2021 were recovered from people's residences throughout 2021 and 2022, and continue to be recovered from residences over the past year, including in the past few months. For example:

- a. On August 2, 2023, in the Northern District of Texas, a search of the defendant's residence allowed the FBI to recover guns, a hat and patch, and cell phone brought by the defendant to the Capitol on January 6, 2021.
- b. On August 8, 2023, agents in the Eastern District of California also searched a residence and recovered a leather vest and painter's mask worn by a suspected rioter. Searches continue to provide evidence of the conduct on that day.
- c. On August 23, 2023, in the Northern District of Illinois, agents searched a residence pursuant to a warrant and recovered the helmet and jacket worn by a suspected rioter on January 6, 2021.

- d. On August 30, 2023, in the Western District of Arkansas, agents successfully recovered a red t-shirt worn by the defendant on January 6, 2021, showing Donald Trump flexing his bicep.
- e. On September 8, 2023, in the Eastern District of Michigan, the FBI recovered a red, hooded sweatshirt worn by the defendant inside the U.S. Capitol on January 6, 2021.
- f. On October 9, 2023, in the Western District of Wisconsin, the FBI recovered clothing and gear worn by the defendant on January 6, 2021, including a ballistic vest and helmet, as well as a handwritten note about defecating in Nancy Pelosi's office, and a phone, camera, and computer hard drive.
- g. On October 30, 2023, in the Eastern District of Missouri, the FBI successful searches in two related cases—in which FBI recovered a hat worn on January 6, along with phones and a laptop with January 6, 2021-related information, as well as a helmet and gloves, 3M gas mask, neck gaiter, and backpack worn on January 6, 2021.
- h. On November 9, 2023, in the Northern District of Illinois, the FBI recovered distinctive gloves and a backpack—both worn on January 6, 2021.
- i. The same day, on November 9, 2023, in the District of New Hampshire, the FBI recovered a jacket and t-shirt that had been worn on January 6, 2021.
- j. On November 13, 2023, in the Eastern District of Michigan, the FBI recovered a jacket and backpack worn on January 6, 2021.

- k. On November 21, 2023, in the Northern District of Ohio, the FBI recovered a jacket worn on January 6, as well as a Bluetooth speaker that the defendant carried with him that day.
- l. On November 29, 2023, in the Northern District of Massachusetts, the FBI recovered a window shutter slat stolen from the Capitol as well as a jacket and hat worn on January 6.
- m. On December 12, 2023, in the Eastern District of Tennessee, the FBI recovered black gloves, a grey hoodie, and a backpack—all worn on January 6, 2021.
- n. On December 13, 2023, in the Northern District of West Virginia, the FBI recovered items worn on January 6, 2021, including a camouflage flag, Washington Capitals jersey, and two hats, as well as two Google Pixel phones matching the phone types linked to phones used by the defendant that day.
- o. On December 15, 2023, in the Eastern District of California, the FBI recovered items worn on January 6, 2021, including a Trump flag, as well as a cell phone with pictures taken by the defendant on January 6, 2021 while at the U.S. Capitol.
- p. On December 20, 2023, in the Western District of Washington, the FBI recovered a cell phone which was a replacement phone, obtained by the defendant after January 6, 2021, which still contained relevant pictures and messages from January 6, 2021.

- q. On January 23, 2024 in the District of New Jersey, the FBI recovered a cell phone that was a replacement phone, obtained by the defendant after January 6, 2021, which still contained relevant pictures, videos, and messages from January 6, 2021.
- r. On January 30, 2024, in the Northern District of Ohio, the FBI recovered distinctive clothing, including a plaid jacket, worn by the defendant on January 6, 2021.
- s. Also on January 30, 2024, in the Eastern District of Tennessee, the FBI recovered a black bandana worn by the defendant at the U.S. Capitol on January 6, 2021, as well as sunglasses worn by the defendant while marching to the U.S. Capitol on January 6, 2021.
- t. On February 7, 2024, in the Eastern District of Virginia, the FBI recovered a ballistic helmet, tactical vest, and “battle dress uniform” pants worn by the defendant on January 6, 2021, as well as documents concerning travel to Washington, D.C. on January 6, 2021.
- u. On February 22, 2024, in the Southern District of Florida, the FBI recovered handheld radios carried on January 6, 2021 as well as hats and a scarf worn on January 6, 2021.
- v. On March 8, 2024, in the District of Maryland, the FBI recovered a jacket consistent with the one worn by the defendant on January 6, 2021.

59. I know, based on my training and experience, that people routinely re-wear clothing and accessories, store these items in their homes, and keep them for an extended period. Clothing and accessories consistent with those worn by ESPINOSA on January 6, 2021

constitute evidence of the commission of the offenses discussed herein, in that ESPINOSA can be visually identified as the individual in the photos and videos discussed above, in part through the distinct attire and accessories worn that day.

60. I also know, based on my training and experience, that cell phones are expensive, and people routinely retain their cell phones for many months or years. I also know, based on my training and experience, that people commonly keep their cell phones and other personal digital devices either on or near their person or at their residence.

61. Your affiant also knows that hundreds of people have been arrested in connection to the riot that occurred at the U.S. Capitol on January 6, 2021. During searches of many those people's homes, from early 2021 through present, in multiple jurisdictions, law enforcement has recovered clothing, paraphernalia, tools, and devices that were worn, used, or carried on January 6, 2021.

62. In addition, based on photos and videos of the offenses that date, numerous persons committing the TARGET OFFENSES possessed digital devices that they used to record and post photos and videos of themselves and others committing those offenses, or to communicate with others about the events of January 6, 2021. Further, based on the investigation, numerous persons committing the TARGET OFFENSES possessed digital devices to communicate with other individuals to plan their attendance at the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

63. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices,

such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that evidence of the offense that originally resided on the Subject's cell phone may also be saved to other digital devices within the PREMISES. Moreover, here, as widely reported in the news media related to this matter, many individuals committing the TARGET OFFENSES kept and posted videos, photos, and commentary about their participation in these offenses, essentially bragging about their participation. Based on that, there is also probable cause to believe that evidence related to these offenses may have been transferred to and stored on digital devices beyond the particular digital device the Subject possessed during the offenses.

64. I also know that many individuals, commonly carry electronic devices on their person and in their vehicles as they travel from place to place.

65. Based on my review of ESPINOSA'S phone records, ESPINOSA used a mobile phone to make at least two calls on January 6, 2021—at least approximately 9:32 a.m. and 7:51 p.m. EST, a time period that bookends the time during which there is probable cause to believe he was at the Capitol (and committed the TARGET OFFENSES) on January 6, 2021.

66. As described above, there is further evidence that Subject had in his/her possession a digital device while at the U.S. Capitol on January 6, 2021. U.S. Capitol Police surveillance footage and open source videos show ESPINOSA using a mobile device throughout the day on January 6, 2021 (see above Images 7, 9, 13, 18, and 21).

67. Further, based on the investigation, numerous persons committing the TARGET OFFENSES possessed digital devices to communicate with other individuals to plan their attendance in Washington D.C. on January 6, 2021, to coordinate with other participants at the gatherings there that day, and to communicate and post on social media and digital forums about the events of January 6 after they occurred.

68. Moreover, it is well-known that virtually all adults in the United States use mobile digital devices. In a fact sheet from April 7, 2021, The Pew Research Center for Internet & Technology estimated that 97% of Americans owned at least one cellular phone, and that that same 2021 report estimated that 85% of Americans use at least one smartphone. See Mobile Fact Sheet, <https://www.pewresearch.org/internet/fact-sheet/mobile/> (last visited November 27, 2023).

69. On February 26, 2024, the FBI reviewed phone records provided by AT&T regarding the devices used by ESPINOSA for his phone number ending in 1658. The AT&T records show that ESPINOSA has changed his device several times since January 6, 2021, but maintained the same phone number on each device. The property to be searched includes an Apple iPhone 8 Plus, IMEI number 3529770929139326; an Apple iPhone 8 Plus, IMEI number 3529770929139336; an Apple iPhone 8 Plus, IMEI number 3529770929139337; an Apple iPhone 8 Plus, IMEI number 3529770929139345; an Apple iPhone 8 Plus, IMEI number 3529770929139346; an Apple iPhone 8 Plus, IMEI number 3529770929139349; an Apple iPhone 14 ProMax, IMEI number 3529770929139349; and an Apple iPhone ProMax, IMEI number 3560414015435106. Based on my training and experience, I know that, even when individuals obtain new cell phones, they frequently transfer data, including application data, photos, text messages, and contacts, from their old phone to their new phone.

70. The property to be searched also includes laptop computers, mobile phones, and/or tablets owned, used, or controlled by ESPINOSA, including but not limited to the specific devices listed above in paragraph 69, hereinafter the “Device[s].”

TECHNICAL TERMS

Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. “Digital device,” as used herein, includes the following three terms and their respective definitions:

1) A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.

3) “Computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory

storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. “Wireless telephone” (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

c. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as

described above, and personal computers, perform many different functions and save data associated with those functions.

d. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. “Computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol (“IP”) Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. “Internet Service Providers,” or “ISPs,” are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line (“DSL”), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically

charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A “modem” translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A “router” often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. “Domain Name” means the common, easy-to-remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For

example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. “Cache” means the text, image, and graphic files sent to and temporarily stored by a user’s computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. “Peer to Peer file sharing” (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user’s computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file’s hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. “VPN” means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name “virtual private network.” The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. “Encryption” is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. “Malware,” short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain

access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

71. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including violations of 18 U.S.C. §§ 1752(a)(1) and (b)(1)(A) (Entering and Remaining in Restricted Building or Grounds with a Deadly or Dangerous Weapon); 18 U.S.C. § 1752(a)(2) and (b)(1)(A) (Disorderly and Disruptive Conduct in a Restricted Building or Grounds with a Deadly or Dangerous Weapon); 40 U.S.C. § 5104(e)(2)(D) (Disorderly and Disruptive Conduct in a Capitol Building or Grounds); and 40 U.S.C. § 5104(e)(2)(G) (Parading, Picketing, or Demonstrating in a Capitol Building), may use Device(s) to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device(s), documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other “Short Message Service” (“SMS”) messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator’s contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

72. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did

not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This

data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is

not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

73. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a

controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other

digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal

activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

74. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate

search of any such digital devices at the PREMISES. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

75. This warrant permits law enforcement agents to obtain from the person of ESPINOSA (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

76. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

77. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

78. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain devices including those manufactured by Android, Apple, or other manufacturers. In many cases, a user registers for this feature by holding the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

79. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

80. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

81. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that

would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

82. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

83. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the

aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

84. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

85. Law enforcement personnel will commence the execution of this search and seizure warrant upon the PREMISES during daytime hours (between 6:00 a.m. and 10:00 p.m.), as early as practicable. It is anticipated that law enforcement personnel will attempt to image or copy digital information from certain servers on the PREMISES, rather than remove those servers from the premises. Such onsite imaging or copying will minimize disruptions to the use of those servers.

86. From my training and experience, I know that imaging or copying information from servers on the PREMISES can be substantially delayed by various factors which cannot be ascertained or sometimes even anticipated until the actual execution of the warrant. There may, for example, be no system administrator available, willing, or able to assist law enforcement personnel to narrow the search by identifying the virtual or dedicated server(s) on the PREMISES, or the server folders, containing information within the scope of the warrant. There may be terabytes or even petabytes of information to be copied. The network architecture of the servers on the PREMISES or the configuration of the server hardware may affect and delay data transfer speeds. Data encryption and password protections may also significantly delay imaging or copying as law enforcement personnel seek to identify necessary passwords without which imaging or copying on the PREMISES would likely be unachievable. Under some circumstances, data downloads can be interrupted by network or hardware malfunctions or other network or hardware attributes which often necessitates restarting the data downloads from the beginning.

87. For all of the foregoing reasons, I respectfully submit that good cause exists, pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), for authorization to execute the search warrant at any time of the day or night. Law enforcement personnel will commence executing the warrant as near to 6:00 a.m. as practicable. However, given the myriad factors that that may prevent completion of the search and seizure by 10:00 p.m., including those described above, I request authorization to continue the warrant execution past 10:00 p.m., if necessary, until completion of the warrant execution. Suspending the execution at 10:00 p.m. until 6:00 a.m. could compromise data downloads in progress, render stored data subject to alteration or deletion, require securing

the PREMISES during the intervening hours, and prolong the disruption of access to, and use of, the PREMISES and the digital devices being searched.

CONCLUSION



I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

/s/ Malachi C. Nkosi

Malachi C. Nkosi
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on March 25, 2024.

ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 6 Blackberry Road, Apartment B, Derry, New Hampshire (the “PREMISES”), further described as a yellow two-story house with a white door and green shutters (see Image 1 below). Apartment B (circled in red below) is clearly marked as being on the right side of the structure.



Image 1

ATTACHMENT B

Property to be seized

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. §§ 1752(a)(1) (entering or remaining in restricted buildings or grounds); 1752(a)(2) (disorderly and disruptive conduct in a restricted building or grounds); 18 U.S.C. § 1752(b)(1)(A), which enhances the punishment if the person, during and in relation to the above offenses, uses or carries a deadly or dangerous weapon or firearm; and 40 U.S.C. §§ 5104(e)(2)(D) (disorderly or disruptive conduct in the Capitol Buildings) and 5104(e)(2)(G) (parading, demonstrating, or picketing in a Capitol Building) (the “TARGET OFFENSES”) that have been committed by Charles Anthony Espinosa (“the Subject”) and other identified and unidentified persons, as described in the search warrant affidavit; including, but not limited to:

- a. Evidence of the commission of the TARGET OFFENSES;
- b. Evidence of any conspiracy, planning, or preparation to commit those offenses;
- c. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
- d. Evidence concerning materials, devices, or tools that were used to unlawfully commit the TARGET OFFENSES;
- e. Evidence of communication devices used in relation to the TARGET OFFENSES;
- f. Evidence of the state of mind of the subject and/or other co-conspirators, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and
- g. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

- h. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
- i. Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;
- j. Evidence concerning the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election and the role and presence of Vice President Pence;
- k. Evidence concerning efforts to obstruct, impede, or disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
- l. Evidence concerning the breach and unlawful entry of the United States Capitol on January 6, 2021;
- m. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;
- n. Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the United States Capitol on January 6, 2021;
- o. Evidence concerning damage to, or theft of, property at the United States Capitol on January 6, 2021;
- p. Evidence concerning awareness that the U.S. Capitol was closed to the public on January 6, 2021;
- q. Evidence of the defendant's presence at the U.S. Capitol on or around January 6, 2021;
- r. Evidence concerning the results of, challenges to, or questions about the legitimacy of the 2020 Presidential Election;
- s. Evidence regarding travel to Washington, D.C. in or around January 2021, motive and intent for travel to Washington, D.C. in or around January 2021, the planning of travel to and activity in Washington, D.C. on or about January 6, 2021, research about the U.S. Capitol, and mode of travel, travel expenses, and travel logistics on or about January 6, 2021.
- t. Evidence regarding the riot at the U.S. Capitol on January 6, 2021;
- u. Clothing and other items that reflect evidence of defendant's presence at the U.S. Capitol on January 6, 2021.

2. Records and information that constitute evidence of identity, including but not limited to:

- a. clothing worn by the subject, to include a leather jacket, red hoodie, black jeans, black shoes, and fingerless gloves;
- b. clothing and other articles that reflect evidence of having participated in the unlawful activity at the U.S. Capitol, including evidence of pepper spray or other non-lethal crowd control remnants;
- c. Other paraphernalia used by or associated with the Subject, to include a large knife with tan handle;

3. Address and/or telephone books and papers reflecting names, addresses and/or telephone numbers, which constitute evidence of conspirators and potential witnesses of violations of the TARGET OFFENSES.

4. Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to:

- a. Any records and/or evidence revealing the Subject's presence at the January 6, 2021, riot;
- b. Any physical records, such as receipts for travel, which may serve to prove evidence of travel of to or from Washington D.C. from November, 2020 through January, 2021;
- c. The Subject's (and others's) motive and intent for traveling to the U.S. Capitol on or about January 6, 2021; and
- d. The Subject's (and others's) activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021.

5. Photographs, in particular photographs of the subject, co-conspirators, or events in Washington D.C. on January 6, 2021, which constitute evidence of the TARGET OFFENSES.

6. Evidence of relationships between members of a conspiracy, including evidence of identification and evidence of motivation to engage in TARGET OFFENSES.

7. Cellular telephones, SIM cards, computers, laptops, I-Pads, DVDs, hard drives, and electronic store devices, and receipts reflecting their ownership and use, which contain records of the commission of the TARGET OFFENSES.

8. Safes, both combination and key type, and their contents, which can contain evidence of the commission of the TARGET OFFENSES.

9. Indicia of ownership, including, receipts, invoices, bills, canceled envelopes, and keys, which provides evidence of identity as to individuals committing the TARGET OFFENSES; and

10. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the “Device(s)”:

- a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
- b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;

- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);
 - e. evidence of the times the Device(s) was used;
 - f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);
 - g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);
 - h. records of or information about Internet Protocol addresses used by the Device(s);
 - i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
11. Routers, modems, and network equipment used to connect computers to the Internet.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from the Subject (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

- (a) any of the Device(s) found at the PREMISES,
- (b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “digital devices” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.